Web Images Videos Maps News Shopping Gmail more ▾

Google scholar [DH eke OR (diffie hellman encrypted key exch] [Search] Advanced Scholar Search
Scholar Preferences

● Search only in Engineering, Computer Science, and Mathematics.
○ Search in all subject areas.

Scholar [ ] - [2003] [include citations] Results **1** - **10** of about **433**. (**0.12** sec)

Did you mean: DH eke OR (diffie hellman ***encryption*** key exchange)

Provably secure password-authenticated **key exchange** using **Diffie-Hellman** - ▶psu.edu [PDF]
V Boyko, P MacKenzie, S Patel - Lecture Notes in Computer Science, 2000 - Springer
... of a standard **key exchange** (eg, **Diffie-Hellman** [15 **...** Following **EKE**, many password authenticated **key exchange** protocols were **...** are working in Z ∗ p . Let **DH**(X, Y **...**
Cited by 329 - Related articles - BL Direct - All 18 versions

Refinement and extension of **encrypted key exchange** - ▶kfupm.edu.sa [PDF]
M Steiner, G Tsudik, M Waidner - ACM SIGOPS Operating Systems Review, 1995 - portal.acm.org
... It requires 5 messages and 5 **encryption** operations over the **...** 3 **EKE** with **Diffie-Hellman** Exponential **Key Exchange ... EKE** variant (referred to as **EKE-DH** from here on **...**
Cited by 193 - Related articles - BL Direct - All 6 versions

Strong password-only authenticated **key exchange** - ▶psu.edu [PDF]
DP Jablon - ACM SIGCOMM Computer Communication Review, 1996 - portal.acm.org
... DH-EKE (**Diffie-Hellman Encrypted Key Exchange**) is the simplest of a number of methods described in [BM92]. The method can also be divided into two stages. **...**
Cited by 360 - Related articles - BL Direct - All 14 versions

Diffie-Hellman key distribution extended to group communication - ▶kfupm.edu.sa [PDF]
M Steiner, G Tsudik, M Waidner - Proceedings of the 3rd ACM conference on Computer …, 1996 - portal.acm.org
... It has been almost twenty years since **Diffie-Hellman** (**DH**) a-party **key exchange** was first proposed in [l]. In the mean- time, there have been many attempts to **...**
Cited by 467 - Related articles - All 5 versions

[PDF] ▶**Encrypted key exchange**: Password-based protocols secure against dictionary attacks
SM Bellovin, M Merritt - Proceedings of the IEEE Symposium on Research in …, 1992 - cse.iitm.ac.in
... for other services, a Id Kerberos [l]. This protocol, known as **encrypted key exchange**, or **EKE**, protects the password from off-line “dictionary” attacks. **...**
Cited by 820 - Related articles - View as HTML - All 15 versions

Extended password **key exchange** protocols immune to dictionary attack - ▶psu.edu [PDF]
D Jablon - Proc. of WET-ICE, 1997 - doi.ieeecomputersociety.org
... plain-text for E,. The symmetric **encryption** can be a **...** S.2 These goals restrict the **Diffie-Hellman** parameters used in SPEKE, and more severely in **DH-EKE**. **...**
Cited by 138 - Related articles - All 16 versions

Password-authenticated **key exchange** between clients with different passwords - ▶iitm.ac.in [PDF]
JW Byun, IR Jeong, **DH** Lee, CS Park - Lecture notes in computer science, 2002 - Springer

... as PA-ENC-**DH** by applying the **DH-EKE** scheme to **...** However PA-ENC-**DH** scheme only considered single **...** logarithm assump- tion(DLA) and the **Diffie-Hellman** assumption(DHA **...**
Cited by 67 - Related articles - BL Direct - All 11 versions

Authenticated **key exchange** secure against dictionary attacks - ▶psu.edu [PDF]
M Bellare, D Pointcheval, P Rogaway - Lecture Notes in Computer Science, 2000 - Springer
... who also offer a protocol, **Encrypted Key Exchange** (**EKE**), and some **...** center of Bellovin and Merritt's **Diffie-Hellman** based **Encrypted Key Exchange** protocol [6 **...**
Cited by 551 - Related articles - BL Direct - All 15 versions

Analysis of **key-exchange** protocols and their use for building secure channels - ▶psu.edu [PDF]
R Canetti, H Krawczyk - Lecture Notes in Computer Science, 2001 - Springer
... this way may be the exponent x used by a party to compute a value g x in a **Diffie-Hellman key-exchange** protocol, or the random bits used to **encrypt** a quantity **...**
Cited by 380 - Related articles - BL Direct - All 14 versions

SIGMA: The 'SIGn-and-MAc'approach to authenticated **Diffie-Hellman** and its use in the IKE ... - ▶iacr.org [PDF]
H Krawczyk - Advances in Cryptography-CRYPTO, 2003 - Springer
... use the acronym **DH** to denote **Diffie-Hellman**, and use **...** in the later case, the **DH** parameters need **...** between the brackets under a symmetric **encryption** function using **...**
Cited by 106 - Related articles - All 5 versions

Did you mean to search for: DH eke OR (diffie hellman ***encryption*** key exchange)

Goooooooooogle ▶

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

DH eke OR (diffie hellman encryptec Search

Go to Google Home - About Google - About Google Scholar